This listing of claims will replace all prior versions and listings of claims in the application:

**Listing of Claims:**

1.-80. (Canceled)

81. (Currently Amended) A system ~~as in Claim 7,~~ including:

a first apparatus including

user controls,

a communications port,

a processor,

a memory containing

a first rule, and

a first secure container containing an audio file, said audio file including steganographically encoded information, the first secure container having associated a second rule, the second rule governing, at least in part, access to or other use of at least a portion of the audio file;

hardware and/or software used for receiving and opening secure containers, said secure containers each including the capacity to contain at least one governed item, at least one rule being associated with each of said secure containers;

a protected processing environment at least in part protecting at least some information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware and/or software used for applying said first rule and said second rule in combination to at least in part govern at least one aspect of access to or use of said audio file; and

hardware and/or software used for transmission of secure containers to other apparatuses and/or for the receipt of secure containers from other apparatuses.

82. (Original) A system as in Claim 81, said steganographically encoded information including at least one electronic fingerprint.

83. (Original) A system as in Claim 81, said steganographically encoded information including a first portion encoded using a first steganographic encoding technique and a second portion encoded using a second steganographic encoding technique.

84. (Original) A system as in Claim 83, in which said first steganographic encoding technique provides a higher degree of security than said second steganographic encoding technique.

85. (Original) A system as in Claim 84, in which at least a portion of said steganographically encoded information is encrypted.

86. (Original) A system as in Claim 83, in which said first portion is encrypted using a first technique which differs in at least one respect from a second encryption technique used for encryption of said second portion.

87. (Original) A system as in Claim 86, in which said encryption techniques differ in at least the key used for each technique.

88. (Original) A system as in Claim 86, in which said encryption techniques differ in the strength of encryption used.

89. (Original) A system as in Claim 81, in which said steganographic encoding includes at least the creation of slight variances in spacings between words or characters, said slight variances encoding at least a portion of said steganographically encoded information.

90. (Original) A system as in Claim 81, in which said steganographic encoding includes at least the creation of slight variances in spacings between lines of text, said slight variances encoding at least a portion of said steganographically encoded information.

91. (Original) A system as in Claim 81, in which said steganographic encoding includes at least the creation of slight variances in the gray scale used in at least a portion of the contents of said first secure container, said slight variances encoding at least a portion of said steganographically encoded information.

92. (Original) A system as in Claim 81, in which said steganographic encoding includes at least the creation of slight variances in the color frequencies used in at least a portion of the contents of said first secure container, said slight variances encoding at least a portion of said steganographically encoded information.

93.-206. (Canceled)

207. (Currently Amended) A system ~~as in Claim 133~~ including:

a first apparatus including

user controls,

a communications port,

a processor,

a memory containing

a first rule, and

a first secure container containing a video file, said video file including steganographically encoded information, the first secure container having associated a second rule, the second rule governing, at least in part, access to or other use of at least a portion of the video file;

hardware and/or software used for receiving and opening secure containers, said secure containers each including the capacity to contain at least one governed item, at least one rule being associated with each of said secure containers;

a protected processing environment at least in part protecting at least some information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware and/or software used for applying said first rule and said second rule in combination to at least in part govern at least one aspect of access to or use of said video file; and

hardware and/or software used for transmission of secure containers to other apparatuses and/or for the receipt of secure containers from other apparatuses.

208. (Original) A system as in Claim 207, said steganographically encoded information including at least one electronic fingerprint.

209. (Original) A system as in Claim 207, said steganographically encoded information including a first portion encoded using a first steganographic encoding technique and a second portion encoded using a second steganographic encoding technique.

210. (Original) A system as in Claim 209, in which said first steganographic encoding technique provides a higher degree of security than said second steganographic encoding technique.

211. (Original) A system as in Claim 210, in which at least a portion of said steganographically encoded information is encrypted.

212. (Original) A system as in Claim 209, in which said first portion is encrypted using a first technique which differs in at least one respect from a second encryption technique used for encryption of said second portion.

213. (Original) A system as in Claim 212, in which said encryption techniques differ in at least the key used for each technique.

214. (Original) A system as in Claim 212, in which said encryption techniques differ in the strength of encryption used.

215. (Original) A system as in Claim 207, in which said steganographic encoding includes at least the creation of slight variances in spacings between words or characters, said slight variances encoding at least a portion of said steganographically encoded information.

216. (Original) A system as in Claim 207, in which said steganographic encoding includes at least the creation of slight variances in spacings between lines of text, said slight variances encoding at least a portion of said steganographically encoded information.

217. (Original) A system as in Claim 207, in which said steganographic encoding includes at least the creation of slight variances in the gray scale used in at least

a portion of the contents of said first secure container, said slight variances encoding at least a portion of said steganographically encoded information.

218. (Original) A system as in Claim 207, in which said steganographic encoding includes at least the creation of slight variances in the color frequencies used in at least a portion of the contents of said first secure container, said slight variances encoding at least a portion of said steganographically encoded information.

219.-332. (Canceled)

333. (Currently Amended) A system ~~as in Claim 259~~ including:

a first apparatus including

user controls,

a communications port,

a processor,

a memory containing

a first rule, and

a first secure container containing an image file, said image file including steganographically encoded information, the first secure container having associated a second rule, the second rule governing, at least in part, access to or other use of at least a portion of the image file;

hardware and/or software used for receiving and opening secure containers, said secure containers each including the capacity to contain at least one governed item, at least one rule being associated with each of said secure containers;

a protected processing environment at least in part protecting at least some information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware and/or software used for applying said first rule and said second rule in combination to at least in part govern at least one aspect of access to or use of said image file; and

hardware and/or software used for transmission of secure containers to other apparatuses and/or for the receipt of secure containers from other apparatuses.

334. (Original) A system as in Claim 333, said steganographically encoded information including at least one electronic fingerprint.

335. (Original) A system as in Claim 333, said steganographically encoded information including a first portion encoded using a first steganographic encoding technique and a second portion encoded using a second steganographic encoding technique.

336. (Original) A system as in Claim 335, in which said first steganographic encoding technique provides a higher degree of security than said second steganographic encoding technique.

337. (Original) A system as in Claim 336, in which at least a portion of said steganographically encoded information is encrypted.

338. (Original) A system as in Claim 335, in which said first portion is encrypted using a first technique which differs in at least one respect from a second encryption technique used for encryption of said second portion.

339. (Original) A system as in Claim 338, in which said encryption techniques differ in at least the key used for each technique.

340. (Original) A system as in Claim 338, in which said encryption techniques differ in the strength of encryption used.

341. (Original) A system as in Claim 333, in which said steganographic encoding includes at least the creation of slight variances in spacings between words or characters, said slight variances encoding at least a portion of said steganographically encoded information.

342. (Original) A system as in Claim 333, in which said steganographic encoding includes at least the creation of slight variances in spacings between lines of text,

said slight variances encoding at least a portion of said steganographically encoded information.

343. (Original) A system as in Claim 333, in which said steganographic encoding includes at least the creation of slight variances in the gray scale used in at least a portion of the contents of said first secure container, said slight variances encoding at least a portion of said steganographically encoded information.

344. (Original) A system as in Claim 333, in which said steganographic encoding includes at least the creation of slight variances in the color frequencies used in at least a portion of the contents of said first secure container, said slight variances encoding at least a portion of said steganographically encoded information.

345.-458. (Canceled)

459. (Currently Amended) A system ~~as in Claim 403~~ including:

a first apparatus including,

user controls,

a communications port,

a processor,

a memory containing

a first rule, and

a first secure container containing a text file, said text file including steganographically encoded information, the

first secure container having associated a second rule, the second rule governing, at least in part, access to or other use of at least a portion of the text file;

hardware and/or software used for receiving and opening secure containers, said secure containers each including the capacity to contain at least one governed item, at least one rule being associated with each of said secure containers;

a protected processing environment at least in part protecting at least some information contained in said protected processing environment from tampering by a user of said first apparatus, said protected processing environment including hardware and/or software used for applying said first rule and said second rule in combination to at least in part govern at least one aspect of access to or use of said text file; and

hardware and/or software used for transmission of secure containers to other apparatuses and/or for the receipt of secure containers from other apparatuses.

460. (Original) A system as in Claim 459, said steganographically encoded information including at least one electronic fingerprint.

461. (Original) A system as in Claim 459, said steganographically encoded information including a first portion encoded using a first steganographic encoding technique and a second portion encoded using a second steganographic encoding technique.

462. (Original) A system as in Claim 461, in which said first steganographic encoding technique provides a higher degree of security than said second steganographic encoding technique.

463. (Original) A system as in Claim 462, in which at least a portion of said steganographically encoded information is encrypted.

464. (Original) A system as in Claim 461, in which said first portion is encrypted using a first technique which differs in at least one respect from a second encryption technique used for encryption of said second portion.

465. (Original) A system as in Claim 464, in which said encryption techniques differ in at least the key used for each technique.

466. (Original) A system as in Claim 464, in which said encryption techniques differ in the strength of encryption used.

467. (Original) A system as in Claim 459, in which said steganographic encoding includes at least the creation of slight variances in spacings between words or

characters, said slight variances encoding at least a portion of said steganographically encoded information.

468. (Original) A system as in Claim 459, in which said steganographic encoding includes at least the creation of slight variances in spacings between lines of text, said slight variances encoding at least a portion of said steganographically encoded information.

469. (Original) A system as in Claim 459, in which said steganographic encoding includes at least the creation of slight variances in the gray scale used in at least a portion of the contents of said first secure container, said slight variances encoding at least a portion of said steganographically encoded information.

470. (Original) A system as in Claim 459, in which said steganographic encoding includes at least the creation of slight variances in the color frequencies used in at least a portion of the contents of said first secure container, said slight variances encoding at least a portion of said steganographically encoded information.

471.-510. (Canceled)